# ETSI EN 302 409 V7.0.3 (2000-08)

*European Standard (Telecommunications series)*

**Digital cellular telecommunications system (Phase 2+); Specification of the Cordless Telephony System Subscriber Identity Module for both Fixed Part and Mobile Station (GSM 11.19 version 7.0.3 Release 1998)**


Reference
DEN/SMG-091119Q7

Keywords
Digital cellular telecommunications system,
Global System for Mobile communications
(GSM), GSM Cordless Telephony System (CTS)

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

# Contents

# Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

# Foreword

This European Standard (Telecommunications series) has been produced by ETSI Technical Committee Special Mobile Group (SMG).

The present document was submitted to Public Enquiry with the ETSI number 301 409. For Vote the number was changed to 302 409 because the number 301 409 is reserved and was allocated accidentally.

The present document defines the interface between the Fixed Part Subscriber Identity Module (FP-SIM) and the Cordless Telephony System Fixed Part Equipment (CTS-FPE) within the digital cellular telecommunications system.

The contents of the present document are subject to continuing work within SMG and may change following formal SMG approval. Should SMG modify the contents of the present document it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version 7.x.y

where:

- 7 indicates GSM Release 1998 of Phase 2+
- x the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- y the third digit is incremented when editorial only changes have been incorporated in the specification..

| National transposition dates | |
|---|---|
| Date of adoption of this EN: | 21 July 2000 |
| Date of latest announcement of this EN (doa): | 31 October 2000 |
| Date of latest publication of new National Standard or endorsement of this EN (dop/e): | 30 April 2001 |
| Date of withdrawal of any conflicting National Standard (dow): | 30 April 2001 |

# 1 Scope

The present document defines the aspects of the internal organization of the FP-SIM which are related to the CTS initialization and CTS enrolment operation phase of CTS as well as the files contained in the SIM for dedicated CTS operation. This is to ensure interoperability between a FP-SIM and a CTS-FPE independently of the respective manufacturers and operators.

The present document defines:

- the contents of the files required for the CTS application*;*
- the application protocol.

All information regarding the interface between the Fixed Part Subscriber Identity Module (FP-SIM) and the Cordless Telephony System Fixed Part Equipment (CTS-FPE) mentioned below are fully compliant with the TS-GSM11.11 [12] unless otherwise stated in the present document.

- the requirements for the physical characteristics of the FP-SIM, the electrical signals and the transmission protocols*;*
- the model which shall be used as a basis for the design of the logical structure of the FP-SIM*;*
- the security features*;*
- the interface functions*;*
- the commands.

For more details regarding CTS, refer to specifications GSM 02.56 [3]and GSM 03.56 [6].

The present document does not specify any aspects related to the administrative management phase. Any internal technical reallocation of either the FP-SIM or the CTS-FPE are only specified where these reflect over the interface. It does not specify any of the security algorithms which may be used.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.
- For this Release 1998 document, references to GSM documents are for Release 1998 versions (version 7.x.y).

[1] GSM 01.02: "Digital cellular telecommunications system (Phase 2+); General description of a GSM Public Land Mobile Network (PLMN)".

[2] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms ".

[3] GSM 02.56: "Digital cellular telecommunications system (Phase 2+); GSM Cordless Telephone System (CTS) Phase 1; Service Description; Stage 1 ".

[4] GSM 03.03: " Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification ".

[5] GSM 03.20: " Digital cellular telecommunications system (Phase 2+); GSM Cordless Telephony System (CTS), (Phase 1) Security related network functions; Stage 2".

[6] GSM 03.56: "Digital cellular telecommunications system (Phase 2+); GSM Cordless Telephone System (CTS), Phase 1; CTS Architecture Description; Stage 2 ".

[7] GSM 04.08: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification".

[8] GSM 04.56: "Digital cellular telecommunications system (Phase 2+); GSM Cordless Telephone System (CTS) Phase 1; CTS radio interface layer 3 specification"

[9] GSM 05.05: "Digital cellular telecommunications system (Phase 2+); Radio Transmission and Reception".

[10] GSM 05.08: "Digital cellular telecommunications system (Phase 2+); Radio subsystem link control".

[11] GSM 05.56: "Digital cellular telecommunications system (Phase 2+), GSM Cordless Telephony System Phase 1 CTS FP radio sub-system".

[12] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface ".

[13] GSM 11.14: "Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface ".

[14] GSM 11.12: "Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

# 3 Definitions, abbreviations and symbols

## 3.1 Definitions

For the purposes of the present document, the following definition applies. For further information and definitions refer to GSM 01.02 [1] and GSM 11.11 [12].

**CTS session:** That part of the card session dedicated to the CTS operation.

## 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply, in addition to those listed in GSM 01.04 [2] and GSM 11.11 [12]:

| | |
|---|---|
| B5 | CTS message authentication algorithm (for the authentication of the CTS-FPE by the CTS-SN) |
| CTS | Cordless Telephony System |
| CTS_MS_Max_TXPWR: | Maximum Output Power at CTS-MS |
| CTS_RXLEV_ACCESS_MIN: | Minimum received signal level to access CTS FP |
| CTSBCH | CTS-Beacon Channel |
| CTS-FP | CTS-Fixed Part (comprises a CTS-FPE and a FP-SIM) |
| CTS-FPE | CTS-Fixed Part Equipment |
| CTSMSI | Temporary Identity of a CTS MS for a given CTS FP |
| CTS-SN | CTS-Service Node |
| FP | Fixed Part |
| FPBI | Fixed Part Beacon Identity |
| FP-SIM | Fixed Part SIM |
| IFPEI | International Fixed Part Equipment Identity |
| Ka | local Authentication Key |

| | |
|---|---|
| $Ki_{FP}$ | CTS Subscriber authentication key; the cryptographic key used by the authentication algorithm, A3, and cipher key generator, A8 |
| Kop | Cryptographic key; used by the cipher B5 |
| MS-SIM | Mobile Station SIM |

## 3.3 Symbols

For the purposes of the present document, the following symbols apply:

| | |
|---|---|
| '0' to '9' and 'A' to 'F' | The sixteen hexadecimal digits |

# 4 Specification of the Fixed Part Subscriber Identity Module

## 4.1 Physical characteristics

GSM 11.11 [12] and GSM 11.12 [14] applies.

## 4.2 Electronic signals and transmission protocols

GSM 11.11 [12] applies.

## 4.3 Logical Model

GSM 11.11 [12] applies with the following additional files IDs reserved for use by CTS:

Dedicated Files**:**

- operational use**:**

  '7F 23' ($DF_{FP\ CTS}$)

Elementary Files**:**

- administration use**:**

  '2F E2' ($EF_{ICCID}$) is a common file between a GSM SIM and a FP-SIM.

## 4.4 Security features

The security aspects of CTS are described in the normative references GSM 03.20 , Annex E [5]. This clause gives information related to security features supported by the FP-SIM to enable the following:

- authentication of the CTS subscriber identity to the network;
- file access conditions.

### 4.4.1 CTS-FPE Authentication for local security system

This subclause describes the authentication mechanism which are invoked by the fixed network interface for operator control on the CTS system. For the specification of the corresponding procedures across the FP-SIM/CTS-FPE interface see clause 4.8.

The CTS-SN sends a Random Number (RAND) to the CTS-FPE. The CTS-FPE passes the RAND to the FP-SIM in the command RUN GSM ALGORITHM. The FP-SIM returns the Kop value to the CTS-FPE which are derived using the algorithms and processes given below. Then the CTS-FPE performs the authentication using Kop and a fixed value to generate the signature SRES. CTS-FPE sends SRES to the network. The fixed network compares this value with the value of SRES which it calculates by itself. The comparison of these SRES values provides the authentication.

A subscriber authentication key $Ki_{FP}$ is used in this procedure. This key $Ki_{FP}$ has a length of 128 bits and is stored within the FP-SIM in the same way Ki is used in the SIM card for GSM authentication.

### 4.4.2 Algorithms and processes

The names and parameters of the algorithms supported by the FP-SIM are defined in GSM 03.20, Annex E [5]. These are:

- Algorithm A3 to generate the first part of the key Kop (Kop1);
- Algorithm A8 to generate the second part of the key Kop (Kop2).

These algorithms may exist either discretely or combined (into A38) within the FP-SIM. In either case the output on the FP-SIM/CTS-FPE interface is 12 bytes. The inputs to both A3 and A8, or A38, are $Ki_{FP}$ (128 bits) internally derived in the FP-SIM, and RAND (128 bits) across the FP-SIM/CTS-FPE interface. The output is the concatenation of Kop1 (32 bits)/Kop2 (64 bits) to produce Kop the coding of which is defined in the command RUN GSM ALGORITHM in subclause 4.6.1.

## 4.5 Description of the functions

GSM 11.11 [12] applies with the following additional specification.

### 4.5.1 RUN GSM ALGORITHM

This function is used during the procedure for authenticating the CTS-FPE to a CTS-SN and to calculate a cipher key. The card runs the specified algorithms A3 and A8 using a 16 byte random number and the subscriber authentication key $Ki_{FP}$, which is stored in the FP-SIM. The function returns the key Kop.

The function shall not be executable unless $DF_{FP\ CTS}$ or any sub-directory under $DF_{FP\ CTS}$ has been selected as the Current Directory. The CHV1 shall be always disabled.

Input:

- RAND.

Output:

- Kop.

## 4.6 Description of the commands

GSM 11.11 [12] applies.

### 4.6.1 RUN GSM ALGORITHM

| COMMAND | CLASS | INS | P1 | P2 | P3 |
|---|---|---|---|---|---|
| RUN GSM ALGORITHM | 'A0' | '88' | '00' | '00' | '10' |

Command parameters/data:

| Byte(s) | Description | Length |
|---|---|---|
| 1 - 16 | RAND | 16 |

Response parameters/data:

| Byte(s) | Description | Length |
|---|---|---|
| 1 - 4 | Kop1 | 4 |
| 5 - 12 | Kop2 | 8 |

The most significant bit of Kop1 is coded on bit 8 of byte 1. The most significant bit of Kop2 is coded on bit 8 of byte 5.

# 4.7 Contents of the Elementary Files (EF)

This clause specifies the EFs for the CTS session defining access conditions, data items and coding. A data item is a part of an EF which represents a complete logical entity.

EFs or data items having an unassigned value, or, which during the CTS session, are cleared by the CTS-FPE, shall have their bytes set to 'FF'. After the administrative phase all data items shall have a defined value or have their bytes set to 'FF'. If a data item is 'deleted' during a CTS session by the allocation of a value specified in another CTS-TS, then this value shall be used, and the data item is not unassigned.

EFs are mandatory (M) or optional (O). The file size of an optional EF may be zero. All implemented EFs with a file size greater than zero shall contain all mandatory data items. Optional data items may either be filled with 'F', or, if located at the end of an EF, need not exist.

For an overview containing all files see figure 1.

## 4.7.1 Contents of the EF at the MF level

There is only one EF at the MF level.

### 4.7.1.1 $EF_{ICCID}$ (ICC Identification)

GSM11.11 [11] applies.

## 4.7.2 Contents of files at the FP CTS domain level

The EFs in the Dedicated File $DF_{FP\ CTS}$ contain subscription related information.

### 4.7.2.1 $EF_{IFPSI}$ (IFPSI)

This EF contains the International Fixed Part Subscriber Identity (IFPSI).

| Identifier: '6F07' | Structure: transparent | | Mandatory |
|---|---|---|---|
| File size: 9 bytes | | Update activity: low | |
| Access Conditions:<br>READ ALW<br>UPDATE ADM<br>INVALIDATE ADM<br>REHABILITATE ADM | | | |
| Bytes | Description | M/O | Length |
| 1 | length of IFPSI | M | 1 byte |
| 2 - 9 | IFPSI | M | 8 bytes |

- length of IFPSI

  Contents:

  The length indicator refers to the number of significant bytes, not including this length byte, required for the IFPSI.

Coding: according to GSM 03.03 [4].

- IFPSI

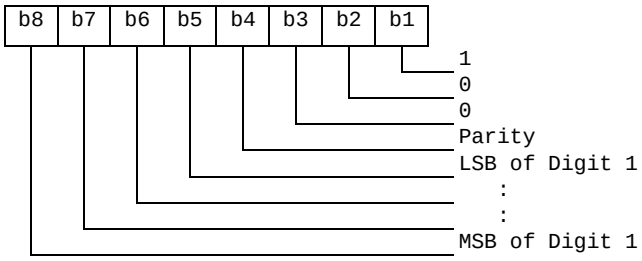
Contents:

International Fixed Part Subscriber Identity.

Coding:

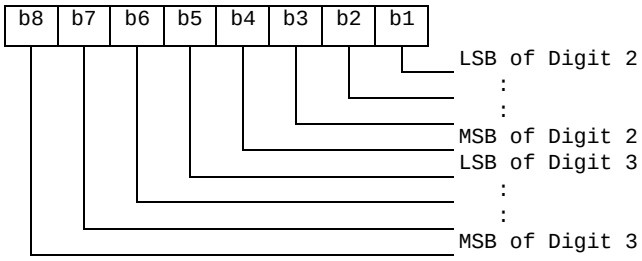
This information element is of variable length. If a CTS operator chooses an IFPSI of less than 15 digits, unused nibbles shall be set to 'F'.

Byte 2:




For the parity bit, see GSM 04.08 [7].

Byte 3:




etc.

### 4.7.2.2 $EF_{CTS\text{-}INFO}$ (CTS information)

This EF indicates the CTS phase of the FP-SIM as well as the CTS services table indicating which of the CTS services are allocated, and whether, if allocated, the service is activated. If a service is not allocated or not activated in the FP-SIM, the CTS-FPE shall not select this service.

| Identifier: '6F38' | Structure: transparent | Mandatory |
|---|---|---|
| File size: X bytes, X ≥ 2 | Update activity: low | |
| Access Conditions:<br>READ ALW<br>UPDATE ADM<br>INVALIDATE ADM<br>REHABILITATE ADM | | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | FP-SIM phase | M | 1 byte |
| 2 | Services n°1 to n°4 | M | 1 byte |
| 3 | Services n°5 to n°8 | O | 1 byte |
| 3 | Services n°9 to n°12 | O | 1 byte |
| etc. | | | |
| X | Services (4X-3) to (4X) | O | 1 byte |

-Services
Contents:
Service n°1: Data download (RFU)
Service n°2: Menu selection
Service n°3: Call control
Service n°4: Proactive SIM

- FP-SIM Phase

Coding:

First byte:
'02': phase 2
'03': phase 2+ and PROFILE DOWNLOAD required (see GSM 11.14 [13]).

Other values are RFU.

If the CTS phase is coded '03' or greater, a CTS-FPE supporting SIM Application Toolkit shall perform the PROFILE DOWNLOAD procedure, as defined in GSM 11.14 [13].

Coding:

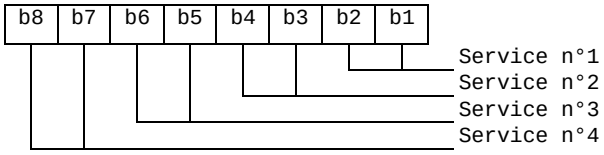
2 bits are used to code each service:
first bit = 1: service allocated
first bit = 0: service not allocated
where the first bit is b1, b3, b5 or b7;
second bit = 1: service activated
second bit = 0: service not activated
where the second bit is b2, b4, b6 or b8.

Service allocated means that the FP-SIM has the capability to support the service. Service activated means that the service is available for the card holder (only valid if the service is allocated).

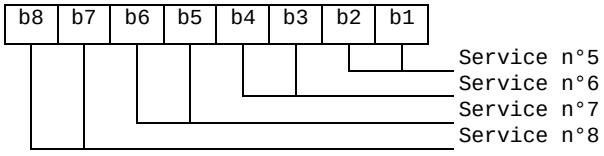
The following codings are possible:
- first bit = 0: service not allocated, second bit has no meaning;
- first bit = 1 and second bit = 0: service allocated but not activated;
- first bit = 1 and second bit = 1: service allocated and activated.

The bits for services not yet defined shall be set to RFU. For coding of RFU see subclause 7.3.

First byte:




Second byte:




etc.

The following example of coding for the first byte means that service n°1 "Data Download" is allocated but not activated:

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 |
|---|---|---|---|---|---|---|---|
| X | X | X | X | X | X | 0 | 1 |

### 4.7.2.3 $EF_{CTS-SNDN}$ (CTS Service Node Dialling Number)

This EF contains the dialling number of the CTS-SN related to a CTS-FPE.

| Identifier: '6F41' | Structure: linear fixed | Mandatory |
|---|---|---|
| Record length: 14 bytes | Update activity: high | |

Access Conditions:

| | |
|---|---|
| READ | ALW |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Length of CTS-Service Number | M | 1 byte |
| 2 | TON and NPI | M | 1 byte |
| 3 to 12 | CTS-SN Dialling Number | M | 10 bytes |
| 13 | Capability/Configuration Identifier | M | 1 byte |
| 14 | Extension Record Identifier | M | 1 byte |

- Length of CTS service number

  Contents:

  this byte gives the number of bytes of the following two data items containing actual BCD number information. This means that the maximum value is 11, even when the actual CTS-SN information length is greater than 11. When a CTS-SN has extension, it is indicated by the extension1 identifier being unequal to 'FF'. The remainder is stored in the $EF_{CTS-EXT}$ with the remaining length of the additional data being coded in the appropriate additional record itself. (see TS-GSM11.11 [12]).

  Coding:

  according to GSM 04.08 [7].

- TON and NPI

  Contents:

  Type of number (TON) and numbering plan identification (NPI).

  Coding:

  according to GSM 04.08 [7].

### 4.7.2.4 $EF_{CTS-CCP}$ (CTS-Capability configuration parameters)

This EF contains parameters of required network and bearer capabilities and CTS-FPE configurations associated with a call established using the service number.

| Identifier: '6F3D' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: 14 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | ALW |
| UPDATE | ALW |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to 10 | Bearer capability information element | M | 10 bytes |
| 11 to 14 | Bytes reserved - see below | M | 4 bytes |

- Bearer capability information element

  Contents and Coding:

  see GSM 04.08 [7]. The Information Element Identity (IEI) shall be excluded, i.e. the first byte of the $EF_{CTS-CCP}$ record shall be length of the bearer capability contents.

  - Bytes 11-14 shall be set to 'FF' and shall not be interpreted by the CTS-FPE.

### 4.7.2.5 $EF_{CTS-EXT}$ (CTS-Extension)

This EF contains extension data of a Service Number. Extension data is caused by:

- a service number which is greater than the 20 digit capacity of the CTS-SN Elementary File or where common digits are required to follow an dialling number of less than 20 digits. The remainder is stored in this EF as a record, which is identified by a specified identification byte inside the CTS-SNDN Elementary File. The CTS-EXT record in this case is specified as additional data;

- an associated called party subaddress. The CTS-EXT record in this case is specified as subaddress data.

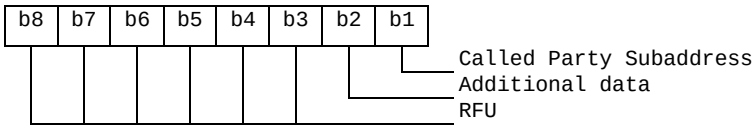
| Identifier: '6F4A' | Structure: linear fixed | Optional |
|---|---|---|
| Record length: 13 bytes | Update activity: low | |
| Access Conditions:<br>READ ALW<br>UPDATE ADM<br>INVALIDATE ADM<br>REHABILITATE ADM | | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Record type | M | 1 byte |
| 2 to 12 | Extension data | M | 11 bytes |
| 13 | Identifier | M | 1 byte |

- Record type

  Contents: type of the record

  Coding:




  b3-b8 are reserved and set to 0;
  a bit set to 1 identifies the type of record;
  only one type can be set;
  '00' indicates the type "unknown".

  The following example of coding means that the type of extension data is "additional data":

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

- Extension data

  Contents: Additional data or Called Party Subaddress depending on record type.

Coding:

Case 1, Extension1 record is additional data:
The first byte of the extension data gives the number of bytes of the remainder of dialling number. The coding of remaining bytes is BCD, according to the coding of dialling number. Unused nibbles at the end have to be set to 'F'. It is possible if the number of additional digits exceeds the capacity of the additional record to chain another record inside the CTS-EXT Elementary File by the identifier in byte 13.

Case 2, Extension1 record is Called Party Subaddress:
The subaddress data contains information as defined for this purpose in GSM 04.08 [7]. All information defined in GSM 04.08 [7], except the information element identifier, shall be stored in the FP-SIM. The length of this subaddress data can be up to 22 bytes. In those cases where two extension records are needed, these records are chained by the identifier field. The extension record containing the first part of the called party subaddress points to the record which contains the second part of the subaddress.

- Identifier

Contents: identifier of the next extension record to enable storage of information longer than 11 bytes.

Coding: record number of next record. 'FF' identifies the end of the chain.

Example of a chain of extension records being associated to an dialling number. The extension1 record identifier (Byte 14+X) of dialling number is set to 3.

| No of Record | Type | Extension Data | Next | Record |
|---|---|---|---|---|
| : | : | : | : | |
| : | : | : | : | |
| Record 3 | '02' | xx ……xx | '06' | |
| Record 4 | 'xx' | xx ……xx | 'xx' | |
| Record 5 | '01' | xx ……xx | 'FF' | |
| Record 6 | '01' | xx ……xx | '05' | |
| : | : | : | : | |
| : | : | : | : | |

In this example dialling number is associated to additional data (record 3) and a called party subaddress whose length is more than 11 bytes (records 6 and 5).

### 4.7.2.6 $EF_{PPLMN}$ (Permitted PLMNs)

This EF indicates the CTS supervising security mode required during the CTS enrolment procedure. The remaining information of the file contains the coding for Permitted PLMNs (PPLMN).

- if the status is set to "LOCAL" the local enrolment procedure of a CTS-MS onto a CTS-FP is performed without requiring any authorisation checking of the Permitted PLMN list;

- if the status is set to "ADMINISTRATIVE" the enrolment procedure of a CTS-MS onto a CTS-FP requires that the CTS-FP contacts the CTS-SN in order to get authorisation for enrolling that CTS-MS;

- if the status is set to "LIST" the local enrolment procedure is used only if the CTS-MS subscriber matches with the PLMNs list stored in the file otherwise the administration control enrolment is required.

| Identifier: '6F7B' | Structure: transparent | Mandatory |
|---|---|---|
| File size: 3X+13 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | ALW |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Status | M | 1 byte |
| 2 - 4 | PLMN 1 | M | 3 bytes |
| 5 - 7 | PLMN 2 | M | 3 bytes |
| 8 - 10 | PLMN 3 | M | 3 bytes |
| 11 - 13 | PLMN 4 | M | 3 bytes |
| 14 - 16 | PLMN 5 | O | 3 bytes |
| etc... | ... | | |
| 3X-1 - 3X+1 | PLMN X | O | 3 bytes |

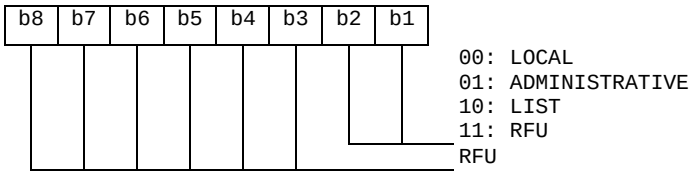
- Status

  Contents:

  CTS Supervising security mode of the CTS enrolment procedure

  Coding:

  Status:




- PLMN

  Contents:

  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

  Coding:

  according to GSM 04.08 [7].

  For instance, using 246 for the MCC and 81 for the MNC and if this is stored in PLMN 3 the contents is as follows:

Bytes 7-9:'42' 'F6' '18'

If storage for fewer than 4 PLMNs is required, the unused bytes shall be set to 'FF'.

### 4.7.2.7 $EF_{AD}$ (Administrative data)

This EF contains information concerning the mode of operation according to the type of FP-SIM, such as normal (to be used by PLMN/PSTN subscribers for CTS operations), type approval (to allow specific use of the CTS-FPE during type approval procedures of e.g. the radio equipment), cell testing (to allow testing of a cell before commercial use of this cell), manufacturer specific (to allow the CTS-FPE manufacturer to perform specific proprietary auto-test in its CTS-FPE during e.g. maintenance phases).

It also provides an indication of whether some CTS-FPE features should be activated during normal operation.

| Identifier: '6FAD' | Structure: transparent | Mandatory |
|---|---|---|
| File size: 3+X bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | ALW |
| UPDATE | ADM |
| INVALIDATE | ADM |
| REHABILITATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | CTS-FP operation mode | M | 1 byte |
| 2 - 3 | Additional information | M | 2 bytes |
| 4 - 3+X | RFU | O | X bytes |

- CTS-FP operation mode

  Contents: mode of operation for the CTS-FP

  Coding:

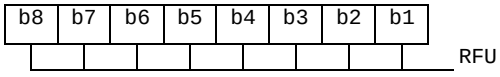
  Initial value
  - normal operation '00'
  - type approval operations '80'
  - normal operation + specific facilities '01'
  - type approval operations + specific facilities '81'
  - maintenance (off line) '02'
  - cell test operation '04'

- Additional information

  Coding:

  - specific facilities (if b1=1 in byte 1);

  Byte 2 (first byte of additional information):



### 4.7.3 Files of CTS

This subclause contains a figure depicting the file structure of the FP-SIM. $DF_{FP\ CTS}$ shall be selected using the identifier '7F23'.

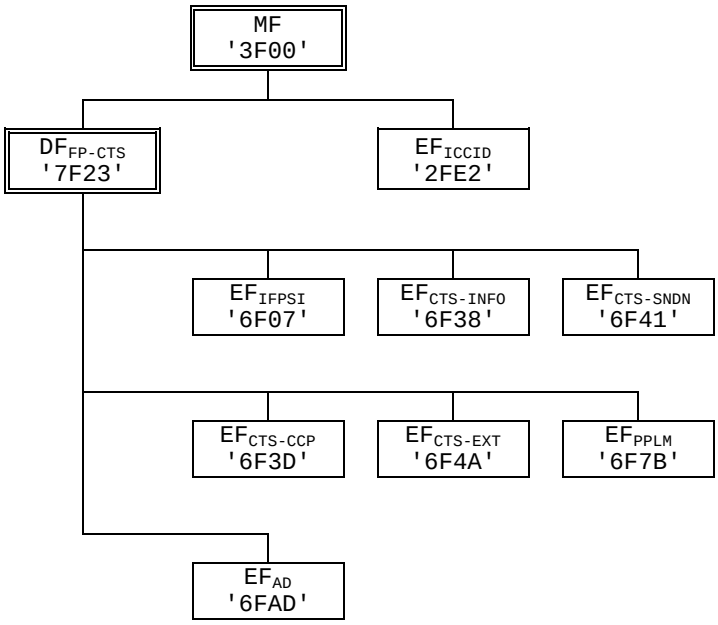



**Figure 1: File identifiers and directory structures of the CTS FP-SIM**

## 4.8 Application protocol

When involved in CTS initialization and/or CTS enrolment operations the FP-SIM interfaces with an CTS-FPE with which messages are exchanged. A message can be a command or a response.

- A CTS command/response pair is a sequence consisting of a command and the associated response.
- A CTS procedure consists of one or more CTS command/response pairs which are used to perform all or part of an application-oriented task. A procedure shall be considered as a whole, that is to say that the corresponding task is achieved if and only if the procedure is completed. The CTS-FPE shall ensure that, when operated according to the manufacturer's manual, any unspecified interruption of the sequence of command/response pairs which realize the procedure, leads to the abortion of the procedure itself.
- A CTS session of the FP-SIM in the CTS application is the interval of time starting at the completion of the FP-SIM initialization procedure and ending either with the start of the CTS session termination procedure, or at the first instant the link between the FP-SIM and the CTS-FPE is interrupted.

During the CTS initialization/enrolment phase, the CTS-FPE plays the role of the master and the FP-SIM plays the role of the slave.

The mandatory services at the FP-SIM/CTS-FPE interface does not require MMI interactions for this stage.

Some procedures are directly caused by the interaction of the CTS-FPE and the CTS-SN using the fixed network. Such procedures are marked " CTS-SN " in the list given below.

Some procedures are automatically initiated by the CTS-FPE. They are marked " CTS-FPE " in the list given below.

The list of procedures at the FP-SIM/CTS-FPE interface in CTS network operation is as follows:

General Procedures:

- Reading an EF CTS-FPE

- Updating an EF CTS-FPE

CTS initialization procedures:

- FP-SIM initialization CTS-FPE
- FP-SIM CTS information request CTS-FPE
- CTS algorithms computation Network

CTS enrolment related procedures:

- IFPSI request Network
- Permitted PLMN information CTS-FPE

SIM Application Toolkit related procedures:

- Data Download Network
- Menu selection CTS-FPE
- Call Control CTS-FPE
- Proactive SIM CTS-FPE

The procedures listed in sub clause 4.8.1 and 4.8.2 are basically required for execution of the normal CTS procedures.

If a procedure is related to a specific service indicated in the CTS Information, it shall only be executed if the corresponding bits denote this service as " allocated and activated ". In all other cases this procedure shall not start.

## 4.8.1 General procedures

### 4.8.1.1 Reading an EF

The CTS-FPE selects the EF and sends a READ command. This contains the location of the data to be read. If the access condition for READ is fulfilled, the FP-SIM sends the requested data contained in the EF to the CTS-FPE. If the access condition is not fulfilled, no data will be sent and an error code will be returned.

### 4.8.1.2 Updating an EF

The CTS-FPE selects the EF and sends an UPDATE command. This contains the location of the data to be updated and the new data to be stored. If the access condition for UPDATE is fulfilled, the FP-SIM updates the selected EF by replacing the existing data in the EF with that contained in the command. If the access condition is not fulfilled, the data existing in the EF will be unchanged, the new data will not be stored, and an error code will be returned.

## 4.8.2 CTS initialization procedures

The CTS initialization is a part of the CTS local security system described in details in GSM 03.20, Annex E [5].

### 4.8.2.1 FP-SIM initialization

After FP-SIM activation (see GSM 11.11 [12]), the CTS-FPE selects the Dedicated File $DF_{FP\ CTS,}$ the CTS-FPE then runs the FP-SIM CTS information request procedure.

For an FP-SIM requiring PROFILE DOWNLOAD, then the CTS-FPE shall perform the PROFILE DOWNLOAD procedure in accordance with GSM 11.14 [13].

Then GSM operation shall start and the CTS-FPE runs the following procedures:

- Administrative Information request;

- IFPSI request;
- CTS-SNDN request;
- Permitted PLMN request.

If the CTS information indicates that the proactive FP-SIM service is active, then from this point onwards, the CTS-FPE, if it supports the proactive FP-SIM service, shall send STATUS commands at least every 30s. The FP-SIM may send proactive commands (see GSM 11.14 [13]), including a command to change the interval between STATUS commands from the CTS-FPE.

After the FP-SIM initialization has been completed successfully, the CTS-FPE is ready for a CTS session.

#### 4.8.2.2 CTS information request

The CTS-FPE performs the reading procedure with $EF_{CTS-INFO}$.

#### 4.8.2.3 Administrative information request .

The CTS-FPE performs the reading procedure with $EF_{AD}$

#### 4.8.2.4 CTS IFPSI request

The CTS-FPE performs the reading procedure with $EF_{IFPSI}$.

#### 4.8.2.5 CTS SNDN request

The CTS-FPE performs the reading procedure with $EF_{CTS-SNDN}$.

#### 4.8.2.6 Permitted PLMN request

The CTS-FPE performs the reading procedure with $EF_{PPLMN}$.

#### 4.8.2.7 FP-SIM Presence Detection and Proactive Polling

As an additional mechanism, to ensure that the FP-SIM has not been removed during a card session, the CTS-FPE sends, at frequent intervals, a STATUS command. A STATUS command shall be issued within all 30 second periods of inactivity on the FP-SIM-CTS-FPE interface. Inactivity in this case is defined as starting at the end of the last communication or the last issued STATUS command. If no response data is received to this STATUS command, then any CTS operation shall not be allowed. If the DF indicated in response to a STATUS command is not the same as that which was indicated in the previous response, or accessed by the previous command, then the CTS-FPE operations shall be terminated as soon as possible but at least within 5 seconds after the response data has been received. This procedure shall be used in addition to a mechanical or other device used to detect the removal of a FP-SIM.

If the CTS-FPE supports the proactive FP-SIM service, and the FP-SIM has this service activated in its CTS information, then during idle mode the CTS-FPE shall send STATUS commands to the FP-SIM at intervals no longer than the interval negotiated with the FP-SIM (see GSM 11.14 [13]).

#### 4.8.2.8 GSM algorithms computation

The CTS-FPE selects $DF_{FP\ CTS}$ and uses the RUN GSM ALGORITHM function (see 6.6.1). The response Kop is sent to the CTS-FPE when requested by a subsequent GET RESPONSE command.

### 4.8.3 CTS enrolment procedures

The CTS initialization is a part of the CTS supervising security system described in details in the GSM 03.20, Annex E [5].

### 4.8.4 SIM Application Toolkit related procedures

For further study.

# 5 Specification of the MS-Subscriber Identity Module:

GSM 11.11[11] applies for all GSM aspects that are not dedicated to CTS

## 5.1 Contents of the EFs at the DF CTS level

The EFs in the Dedicated File $DF_{CTS}$ contain CTS service related information.

### 5.1.1 $EF_{CTS-FPRIP}$ (CTS Fixed Part Radio and Identity Parameters)

This EF contains miscellaneous information which identify each CTS-MS/CTS-FP pair within a record. Two types of information are stored in the file:

Identity parameters:

- FPBI and IFPEI are used to identify a CTS-FP. IFPEI is transmitted by the CTS-FP to the CTS-MS during the enrolment for verification. FPBI is always transmitted by the beacon channel;
- CTS-MSI is a local number to identify a CTS-MS enrolled on a CTS-FP. The CTS-MSI is used when a identity request is sent by the CTS-FP;
- Ka is the CTS authentication key (refer to GSM 03.20, Annex E [5]).

Radio parameters:

- CTSBCH is used by the CTS-FP to allow synchronisation of CTS-MSs. The CTSBCH carrier frequency is issued from the CTS Generic Frequency List (see GSM 05.56, [11]);
- CTS_RXLEV_ACCESS_MIN is the minimum received signal level to access to a CTS-FP;
- CTS_MS_Max_TXPWR is the maximum authorized output power control level that the CTS-MS shall use with a CTS-FP.

| Identifier: '4F01' | Structure: linear fixed | Mandatory |
|---|---|---|
| Record length: X +46 bytes | Update activity: low | |
| Access Conditions:<br>READ CHV1<br>UPDATE CHV1<br>INVALIDATE ADM<br>REHABILITATE ADM | | |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 to X | Alpha Identifier | O | X bytes |
| X+3 | FPBI | M | 3 bytes |
| X+19 | IFPEI | M | 16 bytes |
| X+22 | CTS-MSI | M | 3 bytes |
| X+38 | Ka | M | 16 bytes |
| X+40 | CTSBCH ARFCN | M | 2 bytes |
| X+41 | CTS_RXLEV_ACCESS_MIN | M | 1 byte |
| X+42 | CTS_MS_Max_TXPWR | M | 1 byte |
| X+46 | Bytes reserved - see below | M | 4 bytes |

- Alpha Identifier

  Contents: Alpha-tagging of the associated fixed part

Coding: see GSM 11.11 [10] (e.g., $EF_{ADN}$).

- FPBI

  Coding: As defined in GSM 03.03 [4]

- IFPEI

  Coding: As defined in GSM 03.03 [4]

- CTS-MSI

  Coding: As defined in GSM 03.03 [4]

- Ka

  Coding: The least significant bit of Ka is the least significant bit of the sixteenth byte of the corresponding key. The most significant bit of Ka is the most significant bit of the first byte of the key.

- CTSBCH

  Contents: CTS Beacon channel

  Coding: Absolute Radio Frequency Channel Number as defined in GSM 05.05 [36].

- CTS_RXLEV_ACCESS_MIN

  Coding: As defined in GSM 05.08 [10].

- CTS_MS_Max_TXPWR

  Coding: As defined in GSM 05.05 [9].

  - Bytes reserved shall be set to 'FF' and shall not be interpreted by the ME.

# Annex A (informative): Support of SIM Application Toolkit by CTS-FPE

For further study.

# Annex B (informative): Suggested contents of the CTS MS-SIM EF(s) at pre-personalization

If EFs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

| File Identification | Description | Value |
|---|---|---|
| '4F 01' | CTS FP RIP | 'FF…FF' |

# Annex C (informative): Suggested contents of the CTS FP-SIM EF(s) at pre-personalization

If EFs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

| File Identification | Description | Value |
|---|---|---|
| '2F E2' | ICC identification | operator dependant (see GSM 11.11 [12]) |
| '6F 07' | IFPSI | operator dependant (see GSM 03.03 [4]) |
| '6F 38' | CTS Info | Phase: (see 6.7.2.2)<br>Services: operator dependant (see 6.7.2.2)) |
| '6F 41' | CTS Service Node Dialling Number | 'FF...FF' |
| '6F 3D' | CTS Capability configuration parameters | 'FF...FF' |
| '6F 4A' | CTS Extension | 'FF...FF' |
| '6F 7B' | Permitted PLMNs | Status: operator dependant (see 6.7.2.6)<br>Permitted PLMNs: 'FF…FF' |
| '6F AD' | Administrative Data | Operator dependant (see6.7.2.7) |

# History

| Document history | | | | |
|---|---|---|---|---|
| V7.0.1 | May 1999 | Public Enquiry<br>(as EN 301 409) | PE 9943: | 1999-05-26 to 1999-10-22 |
| V7.0.2 | May 2000 | Vote | V 20000721: | 2000-05-22 to 2000-07-21 |
| V7.0.3 | August 2000 | Publication | | |
| | | | | |
| | | | | |